STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G2: Firewall Security

1. INTRODUCTION:

Firewall Security: An effective combination of hardware, software, and policies used to control traffic between different network security trust levels.

2. OBJECTIVE:

Establish standards for configuring, operating, documenting, and maintaining firewalls.

3. SCOPE:

These guidelines apply to the configuration and operation of all State owned, controlled, and contracted firewall devices utilized in all information systems that receive, process, store, display, or transmit State information regardless of mission impact or data category. They are applicable to all systems regardless of data sensitivity or impact level except where identified otherwise.

This guideline is expected to become a standard, and the recommendations will become requirements, after a (to-be-determined) period of voluntary implementation. Organizations are encouraged to implement these guidelines as soon as practical.

4. GUIDELINES:

Based on the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-41: Guidelines on Firewalls and Firewall Policy, and other best practices, the following recommendations should be applied to the baseline firewall configuration and operation for State of Alabama information systems.

4.1 FIREWALL ARCHITECTURE AND PLACEMENT

Firewalls should be in place at the enclave boundary, managed access points, and appropriate connection points (LAN-to-WAN connections, LAN-to-LAN connections, and WAN-to-WAN connections).

Internet access (if allowed) should be routed through a demilitarized zone (DMZ) or proxy.

When protecting the boundaries of a network, the firewall should be placed between the private network and the perimeter router and the DMZ.

Firewalls should be deployed to monitor and control all approved wireless access protocol (WAP) gateways.

Host-based firewalls should be employed on information systems that provide Remote Access Services (RAS) capabilities. Firewalls should be configured to detect unauthorized access, alert IT staff, and prevent exploitation of network services.

Use application-level gateways or firewalls to proxy all traffic to external networks. Web proxy services should be provided as a minimum. Devices such as SSL Gateways, E-mail Gateways, etc., will proxy services to protect the enclave; therefore, a layer 4 or stateful inspection firewall, in collaboration with application level proxy devices to service all connections, is an acceptable alternative.

4.2 FIREWALL PLATFORM OPERATING SYSTEM CONFIGURATION

Firewall platforms should be implemented on systems containing operating system builds that have been stripped down and hardened for security applications (i.e., a bastion host).

Firewall operating system builds should be based upon minimal feature sets. All unnecessary operating system features should be removed from the build prior to firewall implementation, especially compilers, and the system shall be hardened against attack.

Hardening procedures include the following:

- Remove all unused networking protocols from the firewall operating system build
- Remove or disable any unused network services or applications
- Remove or disable any unused user or system accounts, rename default admin accounts, and apply complex password rules to all user accounts (in accordance with State IT Standard 620-03S1)
- Apply all relevant operating system patches
- Disable or remove from the server chassis any unused physical network interfaces

Ensure the firewall does not utilize or enable any services (DNS, HTTP, etc.) not required by the firewall engine.

Ensure the firewall is configured to protect the network against denial of service attacks (e.g., Ping of Death, TCP SYN floods, etc). If the site has implemented SYN flood protection for the network using the premise router, it is not an additional requirement to implement this on the firewall.

4.3 FILTERING POLICIES

Perimeter filtering rules can be applied to any internal firewall device or router and should be implemented to the fullest extent possible. This is necessary in order to minimize internal threat and protect the enclaves. Allowing only approved IP addresses through the perimeter router will control access to required ports and services.

Before a firewall policy can be created, some form of risk analysis must be performed on the applications that are necessary for accomplishment of the organization’s mission. The Enclave firewall rules should be based on applications being used within the internal Enclave; all non-required ports and services should be blocked by the most restrictive rules possible: a deny-by-default policy (i.e., “that which is not expressly allowed is denied”).

The requirement for perimeter protection necessitates that either a firewall implemented to protect the enclave or the premise router ACLs are in a “deny by default” posture (one or the other will satisfy this requirement for the enclave boundary).

Firewalls should have Access Control Lists (ACL) configured to provide a basic level of access control over network connections based on security or operational policy.

Firewall ACLs should be configured to filter and block ingress and egress services, sources, destinations, and protocols not required or authorized across the enterprise boundary.

The default policy for handling inbound traffic is to block all packets and connections unless the traffic type and connections have been specifically permitted.

The firewall rule set should always block the following types of traffic:

- Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic
- Inbound or Outbound traffic from a system using a source address that falls within the address ranges set aside (in RFC 1918) as being reserved for private networks:

  10.0.0.0 to 10.255.255.255 (Class A, or “/8” in CIDR notation)

  172.16.0.0 to 172.31.255.255 (Class B, or “/12” in CIDR notation)

  192.168.0.0 to 192.168.255.255 (Class C, or “/16” in CIDR notation)
- Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic
- Inbound traffic containing IP Source Routing information
- Inbound or Outbound network traffic containing a source or destination address of 127.0.0.1 (localhost)
- Inbound or Outbound network traffic containing a source or destination address of 0.0.0.0
- Inbound or Outbound traffic containing directed broadcast addresses.

The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address. Do not use “Any” as a service. Use subnets or specific IP addresses for source and destination addresses and use individual services or service groups.

Do not enable NAT for inbound traffic unless it is required by an application. If, for example, NAT is enabled for inbound SMTP traffic, the SMTP server might act as an open relay.

4.4 PUBLIC ACCESS POLICY

Public Access Policy refers to the firewall access control policies that apply to perimeter protection DMZs. Public access in this case is defined as any anonymous packet that originates from outside the state network and is allowed to enter the DMZ. Public access presents the greatest risk to the State of Alabama IT enterprise. Accordingly, these policies will be controlled by Chief Information Officer (CIO) and require CIO approval to modify.

The following protocols will be permitted from anonymous internet protocol (IP) addresses to the DMZ servers. Unless specifically mentioned, all other protocols will be denied access by the firewall.

- HTTP will be permitted from anonymous IP addresses to public web servers on the DMZ.
- Hyper-text transfer protocol secure (HTTPS) will be permitted from anonymous IP addresses to public web servers on the DMZ.
- Simple mail transfer protocol (SMTP) will be permitted from anonymous IP addresses to public e-mail servers on the DMZ. This type of network traffic will be routed through the gateway's anti-virus device before it is sent to public e-mail servers.
- If external FTP services are required, then FTP will be permitted from anonymous IP addresses to public FTP servers on the DMZ.
- If remote users require VPN access to a VPN concentrator, then required ports and protocols will be permitted from anonymous IP addresses to VPN concentrators on the DMZ.

The following protocols will be permitted from DMZ servers to servers within the internal network. Unless specifically mentioned, all other protocols from the DMZ to the internal network will be denied by the firewall.

- If the public web server on the DMZ hosts active content, the Web server may connect to application servers on the internal network using the minimum required protocols to implement the connection. Examples of these protocols may be Netscape Application Programming Interfaces (APIs), Java 2 Platform Enterprise Edition (J2EE), and NET protocols.
- SMTP will be permitted from the e-mail server on the DMZ to e-mail servers on the internal network.
- If a remote access VPN concentrator resides on the DMZ, then a limited set of protocols will be permitted from the VPN concentrator to the internal network. These protocols include post office protocol (POP), internet message access protocol (IMAP) for e-mail; HTTP and HTTPS for web access; Telnet and FTP for system administrators; lightweight directory access protocol (LDAP) for Windows Active Directory login; and network basic input/output system (NETBIOS) protocols for Windows networking.

No protocols will be permitted from DMZ servers to the external network.

The following protocols will be permitted from servers within the internal network to DMZ servers. Unless specifically mentioned, all other protocols from the internal network to the DMZ will be denied by the firewall.

- The secure shell (SSH) protocol will be used to push web content to the public Web server. SSH will be permitted from the internal network to the public web server on the DMZ.
- The SSH protocol will be used to push files to the public FTP server. SSH will be permitted from the internal network to the public FTP server on the DMZ.

The following protocols will be permitted from the internal network to the external network. Unless specifically mentioned, all other protocols from the internal network to the external network will be denied by the firewall.

- DNS will be permitted from internal DNS servers to internet service provider DNS servers. This flexibility will allow name resolution of external IP addresses.
- HTTP and HTTPS with the secure sockets layer (SSL) HTTPS will be permitted from internal network IP addresses to the external network. These protocols will be routed through the web proxy to provide web security.

4.5 IDENTIFICATION & AUTHENTICATION

The firewall should support a secure, strong user authentication system (e.g., Radius or TACACS+).

Ensure the firewall authenticates all administrators using individual accounts before granting access to the firewall's administration interface.

All user and administrator accounts should be assigned the lowest privilege level that allows them to perform their duties.

Ensure the firewall is set to lock out accounts after three unsuccessful logon attempts.

Default firewall passwords must be changed as part of initialization/configuration of any new firewall and every 90 days thereafter or as stipulated in the current State Standards, or immediately after the termination of any employee who has performed firewall administration activities.

4.6 LOGGING & AUDITING

Firewalls should log activity, and firewall administrators should examine the logs daily in accordance with the logging requirements of State IT Standard 670-06S1.

The firewall should provide the ability to record a readable audit log of security-related events, with accurate dates and times, with the capability to search and sort the audit log based on relevant attributes. Enable the following logging capabilities on the firewall:

- Log unsuccessful authentication attempts
- Stamp audit trail data with the date and time when recorded

- Record the Source IP, Destination IP, protocol used, and the action taken
- Log administrator logons, changes to the administrator group, and account lockouts
- Protect audit logs from deletion and modification

The Network Time Protocol (NTP) or another appropriate mechanism should be used to synchronize the logs with other logging systems.

Firewall logs shall be retained in accordance with state log management standards.

Configure the firewall to alert the administrator of a potential attack or system failure.

4.7 ADMINISTRATION/MAINTENANCE

Limit the use of in-band management to situations where the use of out-of-band (OOB) management would hinder operational commitments or when emergency situations arise. Approve the use of in-band management on a case-by-case and documented basis.

Ensure all in-band management connections to the device require passwords.

Ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.

Ensure in-band management access to the device is secured u using a State-approved encryption method (e.g., AES, 3DES, SSH, or SSL).

Ensure the timeout for in-band management access is set for no longer than 10 minutes.

To ensure the proper authorized network administrator is the only one who can access the device, ensure device management is restricted by two-factor authentication (e.g., PKI or alternate token logon).

4.8 VULNERABILITY MANAGEMENT

Firewall applications and host systems must maintain a secure system configuration in accordance with state vulnerability management standards.

Use a supported version of the firewall software with all security-related patches applied.

Subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.

Ensure all firewalls are scanned at least quarterly for vulnerabilities. Document in local procedures the scanning/assessment activities. Generate a Plan of Action and Milestones (POA&M) to correct any findings.

4.9 CONFIGURATION MANAGEMENT (CM)

Proposed changes to the firewall must be evaluated, approved, and documented in accordance with organizational CM processes prior to deployment/implementation.

Evaluation shall include testing of all patches, upgrades, and new applications destined for use on any firewall prior to deployment and assessment for information assurance and accreditation impact prior to implementation.

4.10 BACKUP & RECOVERY

Policies and procedures to routinely or automatically backup, verify, protect, and restore (as required) data (including logs), information systems (including configurations), or devices at every level shall be implemented in accordance with applicable state standards.

All firewalls should be backed up immediately prior to production release.

Firewall configuration data should be backed up weekly and whenever configuration changes occur.

Firewall backups should be performed via an internally situated backup mechanism (e.g., tape drive). Firewall backups shall not be written to any backup servers located on protected networks as this may open a potential security hole to that network.

All firewall backups should be full backups (there is no real need or requirement for incremental backups).

4.11 DOCUMENTATION

Include the following documentation on a network based firewall with other network documentation and in applicable system security plans:

- System hardware list
- System software list
- Documentation, schematics or diagrams depicting the enclave IT configuration/architecture
- Listing of port assignments and their use
- Copy of the security architecture, schematics, or diagrams that depict the security architecture for both the primary as well as any/all alternate sites
- Copies of maintenance support contracts, logs, and documentation
- Copies of documents detailing business continuity plans and arrangements (e.g., operating procedures, Continuity of Operations Plan (COOP), Emergency Plans, Incident Response Plans, Disaster Recovery (DR) Plan (DRP), etc.)
- Configuration Management (CM) Plan, Configuration Control Board (CCB) Charter, and other relevant CM/CCB documentation the system requires
- Procedures for testing and implementing patches, updates, and new applications
- A listing of key computing facilities that house key IT assets, emergency power backup plans, and documentation for the key computing facilities
- The Personnel Training Plan or appropriate documentation that identifies the personnel training requirements

- Copy of the data back-up and restoration policies and procedures

5. DEFINITIONS:

CIDR: Short for Classless Inter-Domain Routing, an IP addressing scheme that replaces the scheme based on classes A, B, and C. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations. CIDR was created to help reduce problems associated with IP address depletion.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 660-02: System Security

6.2 RELATED DOCUMENTS

Information Technology Standard 620-03S1: Authentication - Passwords

Information Technology Standard 670-01S3: Vulnerability Scanning

Information Technology Standard 670-03S1: Vulnerability Management

Information Technology Standard 670-06S1: Log Management

Information Technology Standard 670-07S1: Backup and Recovery

Information Technology Standard 680-03S1: Encryption

Signed by Art Bess, Assistant Director

7. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/30/2008	